Vendor Security Questionnaire

Date	***8/3/2016***	***Company Name***	***Nemaris, Inc.***
Full name	***Steve Schwab***	***Product or Service Name***	***Surgimap***
Title	***Account Executive***	***Website***	***http://surgimapspine.com/***

For any answer found below that alludes to an attached document, note that all the referenced documents can be found on our web site under the Product/IT Department tab by going to http://surgimapspine.com/support/it-department/ and looking through all of our compliance, regulatory, and security posts.

Provide a brief summary of what the product or service will do for Hospital.	Surgimap provides capability of studying spinal deformities and planning better deformity correction. User can upload images from various sources including PACS, creating a copy and manipulate images. This solution will be used to enable the spinal surgeon to improve outcomes and reduce risks.
What is the nature of the data to be processed? Select all that apply	☐ ***Patient Data,*** ☐ ***Credit Card,*** ☐ ***Employee Information,*** ☐ ***Other Sensitive Data, Specify _____*** ☒ ***No Confidential or Sensitive Data***
Which components are included in the product or service? Select all that apply	☒ ***Workstation,*** ☐ **Mobile Devices,** ☐ **Biomedical Devices** ☒ ***Hospital Hosted Server,*** ☐ ***Vendor Hosted Data Center,*** ☐ ***3rd Party Data Center,*** ☐ ***A Cloud Provider Service (SaaS, PaaS, IaaS)*** ☒ ***Other, Specify: Surgimap Software***
What types of documents will be signed as part of the implementation of this product? Select all that apply	☒ ***Formal Contract*** ☐ ***Business Associate Agreement*** ☐ ***Data Use Agreement*** ☒ ***Non-Disclosure Agreement,*** ☐ ***Contract Addendum for security,*** ☐ ***Other, Specify _____***
Approximate # of Users:	***Spine Surgery Department***

Who will support this Application or Service? Select all that apply	☒ ***Vendor,*** ☐**Hospital,** ☐ **Other, Specify _____**

1. **Documentation** Please provide the documentation requested below when submitting this survey. No or N/A answers will require an explanation in the vendor comment(s) field.

#	Document	Attached? (Yes/No, N/A)	Vendor Comment(s)	Hospital Comments
1.1	Vendor's information security policy.	Yes	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode. Details of our security policy can be found in section 4 of our Surgimap-Services-Agreement.pdf	
1.2	Vendor's privacy policy	Yes	All data is encrypted to the user's credentials. Users can only see their own patient images that they loaded into Surgimap. All data and images are owned by the user, no patient data is shared to Surgimap. Details of our security policy can be found in section 4 of our Surgimap-Services-Agreement.pdf	
1.3	User account setup and maintenance process for end users and administrators.	No	After users have downloaded/installed Surgimap software, they can click the "Create An Account" tab and follow the on screen prompts. User will receive an activation email to complete the process of setting up a Surgimap account. Ongoing maintenance, e.g., password reset is managed by the user using in software links. In addition, Surgimap can also provide administrative support. If desired, Surgimap can work with Hospital/Institution staff to create	

			accounts on behalf of the users.	
1.4	Any white papers or product and service configuration guidelines related to security, privacy, or regulatory compliance.	Yes	Surgimap is a medical device and as such is regulated by the FDA and must comply with HIPAA guidelines. Since user credentials are verified before logging into Surgimap, the software needs to authenticate against our AWS solution. Details of our HIPAA Compliance, AWS Security and FDA audits are attached. Relevance documents include: FDA Approval Letter FDA-EIR Findings Surgimap HIPAA Agreement AWS HIPAA Compliance AWS Security Whitepaper	
1.5	Network, data flow and application architecture diagrams for the application. Include any firewall exceptions required to function in Hospital's Network.	No	Surgimap is a free standing ".exe" software and can be downloaded by anyone from www.surgimap.com. There are no interfaces required for it to work at your institution beyond connectivity to the internet for the software download and periodic updates. If desired, user can link their hospital PC to the PACS system via a DICOM node. Likewise, user can sync their local Surgimap work to our AWS cloud solution. There is no additional hardware required to run Surgimap. There is no required data flow beyond download to install the software, sign-up to use.	
1.6	SSAE 16 Type II assessment executive summary. (Required if the vendor or a third party will host confidential Hospital data.)	Yes	Surgimap will store patient images using 256-bit encryption in the user's local (at Hospital) database. In addition, users can synchronize their work to the Surgimap online version stored at Amazon AWS. All data at AWS conforms to SSAE 16 Type II. See attachment titled AWS-Security-Whitepaper.pdf on page 7 under section titled AWS Compliance Program.	
1.7	Please provide your software development lifecycle methodology.	No	As part of the FDA & CE mark process, we have implemented a comprehensive quality management	

			system including a software lifecycle methodology incorporating iterative modular feature development, testing, QA sign-offs.	
1.8	Copy of any security certification or assessments the vendor may have that has a bearing on this security assessment. Such as a PCI-DSS certification, or biomedical device certification from the FDA.	Yes	Surgimap is an FDA medical device with the CE marking as well as TGA approval. Relevant documents include: FDA Approval Letter FDA-EIR Findings EC Certificate	
1.9	Any statement of work or other documentation of contracting work.	No	Surgimap is freeware.	

Security within Hospital's Environment

2. Workstations

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
2.1	Will this product or service function correctly with all of the following:			
2.2a	Third Party and OS patches Hospital determines are necessary, on its own schedule?	Yes	Yes, Surgimap's desktop version is compatible on Microsoft Windows XP and newer & MAC OS 10.7 and newer.	
2.2b	Hospital anti-virus/malware client running on a continuous basis (List all excluded directories)?	Yes	Trend Micro & ESET may require exception added for SurgimapForWindows.exe, Surgimap.exe, Surgimap.app (for MAC)	

2.2c	Hospital host-based firewall or device control client?	Yes	SurgimapForWindows.exe, Surgimap.exe and Surgimap.app (MAC) must be allowed for our desktop version in order to verify user credentials, query images from PACS, as well as to receive periodic software updates. Specifically https://www.surgimap.com/api domain must be allowed along with the following ports: 8080, 80, 443. Please the Surgimap-Connection-Guidelines.pdf for details.	
2.2e	Without the user having local administrative privileges?	Yes	Yes, Surgimap can be run without local admin rights. Note, admin rights may be required for installation.	
2.3	Will sensitive information or other confidential data be deleted from local storage, temp files and memory upon logging out of the application?	No	Surgimap is a complementary software to the surgeon's existing PACS. All original patient images will stay on the PACS system. Surgimap does not delete these originals when imported.	

3. Mobile Devices

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
3.2	Will the product or service function with a mobile device management solution?	Yes	Surgimap runs on Hospital/Institution PCs and all data stays within Surgimap/Hospital. However, there is an optional feature (off by default) letting users sync their work to iOS devices for viewing purposes e.g., OR schedule for upcoming week with surgical pre-op plan and images.	

3.3	Will the product or service function on devices with full drive encryption?	Yes	Surgimap is fully encrypted and in additional will also run on full encryption devices, e.g., FIPS 140-2 media.	

4. Bio Medical Devices ☒ Application does **not** use or interact with Bio Medical Devices.

Item	Question	Yes / No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
4.1	Does your system use 256bit encryption or greater (AES-256) to protect ePHI in transit and at rest?	Yes	Yes, Surgimap runs on Hospital computers. Surgimap uses 256-bit AES encryption for data and 512 bit encryption for images. When connecting to Surgimap to PACS, images will be pushed through Hospital IT environment/network/computers with their own encryption standards.	
4.2	Can Hospital manage updates on the device operating system? If yes, is specialized training required?	Yes	Surgimap runs on Hospital devices.	
4.3	Is this system running on an operating system that is currently supported by the vendor? What OS is the system running?	Yes	Surgimap runs on Hospital devices. Surgimap support Windows XP and higher, MAC OS 10.7 and newer.	

5. Servers ☒ Application does **not** utilize servers on Hospital's network.

Item	Question	Yes / No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments

5.1	Will this product or service function correctly on servers with all of the following?	Yes	Surgimap can run on a Citrix/RDS environment. In addition, Surgimap uses a DICOM node to connect to PACS. Note, this is not a requirement. We recommend running Surgimap on a local PC, however installing on a server is also an option.	
5.1a	Third Party and OS patches Hospital determines are necessary, on its own schedule?	Yes	Surgimap can run on Hospital devices and network.	
5.1b	Hospital anti-virus client running on a continuous basis? (List all excluded directories)	Yes	Surgimap can run on Hospital devices and network.	
5.1c	System backups performed using a method of Hospital's choosing, including encrypting any backups?			
5.1d	Accept vulnerability scans on all servers without disruption?			
5.2	Can systems storing confidential data be located in protected zones that are not in the Hospital DMZ?			
5.3	Can database and applications servers be separated?			
5.4	Can test and production environments run on separate systems?	Yes		
5.5	Will the test environment use non-production data?	Yes		
5.6	Will confidential data stored on the system be encrypted? (If yes, please include the encryption standard//method	Yes	Yes, Surgimap can run on Hospital servers. Surgimap uses 256-bit AES encryption for data and 512 bit encryption for images. When connecting to Surgimap to	

	in the comments section.)		PACS, images will be pushed through Hospital IT environment/network/computers with their own encryption standards.	

6. Remote Support Access ☒Vendor or other Third Party does **not** need remote access into Hospital.

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
6.1	Is the vendor capable of conducting remote support using a Hospital provided SSL VPN rather than 3rd party tools?	Yes	Most Surgimap support can be conducted via phone/email. If required, for us to view the user's screen to verify proper installation, we can use any remote screen viewing tool including VPN access to the user's computer.	
6.2	If you answered no to 6.1 please provide your remote access methodology with documentation, installation and instructions.		In addition to SSL VPN, we use Cisco WebEx Meeting Center as well as TeamViewer for remote support.	

7. Network – Data in Transit

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
7.1	Are all the protocols used by the product or service encrypted in transit? If not please list the unencrypted protocols along with additional	Yes	Yes, Surgimap uses HTTPS for those users who want to synchronize data to our cloud/mobile solution. The PACS DICOM node/data transfer conforms to DICOM standard. For cloud sync to our Amazon solution, AWS MFA supports the use of both hardware tokens and virtual MFA devices.	

	information.		Virtual MFA device use the same protocols as the physical MFA devices, but can run on any mobile hardware device, including smartphones. Details can be found in the AWS Security Whitepaper.pdf document.	
7.2	Will all data in transit outside the Hospital internal network be encrypted? Provide the encryption solution/strength used for data in transit.	Yes	Yes, Surgimap uses HTTPS for those users who want to synchronize data to our cloud/mobile solution. The PACS DICOM node/data transfer conforms to DICOM standard. For cloud sync to our Amazon solution, AWS MFA supports the use of both hardware tokens and virtual MFA devices. Virtual MFA device use the same protocols as the physical MFA devices, but can run on any mobile hardware device, including smartphones. Details can be found in the AWS Security Whitepaper.pdf document.	
7.3	Will this solution require wireless connectivity? If so please provide additional information.	No	Wireless is not required. Surgimap needs internet connectivity for period updates This can be via wired or wireless.	

Application Security

8. Password and Authentication ☒ *Application uses pass-through authentication to Hospital's Active Directory or LDAP*.

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
8.1	Are passwords masked during entry?	Yes		
8.2	Must all passwords have minimum of 8	Yes	Yes, Surgimap minimum password requirements are 8 characters in length, one alpha upper capitalization, one	

	characters? Is this configurable?		alpha lower case, one numeric value, no special characters. Maximum length of 50 characters.	
8.3	Must passwords have 3 of the following 4 characteristics: Alpha upper, Alpha Lower, Numeral, Special Character?	Yes	Yes, Surgimap minimum password requirements are 8 characters in length, one alpha upper capitalization, one alpha lower case, one numeric value, no special characters. Maximum length of 50 characters.	
8.4	Is the maximum number of failed login attempts before the account is locked less than or equal to10 attempts?	Yes	To prevent brute force attacks, users are locked out with 3 failed attempts when in hospital mode.	
8.5	Are accounts locked out for at least 30 minutes after maximum failed login attempts are reached?	Yes	Users are locked out permanently until they can verify their password in online mode against our AWS credentials.	
8.6	Does the system require passwords to be changed after first login and after being reset?	Yes	When a new account is created, users cannot log in until they create a new password. Likewise, when users request a password reset, they must create a new password. User can request a password reset password email to be sent to their email address on file. Once received, user is prompted to create a new password meeting the minimum requires. In addition, users can also change their password by logging into their online user profile settings on www.surgimap.com/access after signing in with original password first.	
8.7	Are passwords encrypted during storage and transmission? (Please include the encryption standard/method in the comments section.)	Yes	Yes, all Surgimap data is encrypted including passwords. All data is encrypted when in flight as well as when stored on Amazon AWS. Amazon uses Multi-Factor Authentication (MFA). Details are in the AWS Security Whitepaper.pdf document.	
8.8	Can the application be configured to time out after a set time of inactivity? Is	Yes	For the desktop version, there is no default time out setting however, this can implemented if required. For our web	

	this a setting the customer can change?		version (Surgimap Access), the default setting is 5 minutes. The mobile version relies on auto-time settings of the user's device.	

9. User Account and Access Management

Item	Question	Yes / No	Vendor Comment (No or N/A answers will require an explanation)	Hospital Comments
9.1	Does the product or service disable default or other generic user accounts? Are all default passwords changed?	No	Surgimap allows multiple users within the same software deployment. Each user signs in with their own credentials (username/password) allowing one or more Hospital workstations to be available to multiple surgeons for image viewing, measuring and outcome simulation.	
9.2	Does user access utilize a role-based access control model?	No	Users do not have roles, they are either inactive or active. Surgimap admins can also disable an account if required by Hospital.	
9.3	Is access based on the least privileged principal?	Yes	Users start with an inactive account. Only upon verification will the user have Surgimap functionality. In addition, for PACS connectivity, users need additional authentication/privileges against Hospital server requirements.	
9.4	Can accounts be modified, created, and disabled, within 8 hours from notification of a change?	Yes	Users can create their own account real time. In addition, Surgimap can also create and disable accounts, real time. Our team is available 8AM to 8PM, Monday to Friday for account changes and will respond within same day on weekends.	
9.6	Does the system support SSO. If so what options are available?	Yes	Surgimap is primarily an application residing on Hospital computers. When configured properly, it allows single sign-	

			on to Surgimap to query PACS systems.	
9.7	Does the system support SAML, ADFS or other Active Directory integration?	No	Not required. Surgimap is standalone application.	
9.8	Does your system support 2nd Factor authentication? If so please provide additional information.	Yes	For users of the Surgimap Access platform, we support 2nd factor authentication as per Amazon AWS. More details in the AWS-Security-Whitepaper.pdf document.	

10. Vulnerability and Patch Management

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
10.1	Are web components tested against OWASP top ten? www.owasp.org	N/A	Users must first authenticate against Hospital computers before reaching Surgimap with its own log in credentials. Surgimap meets/exceeds all the HIPPA requirements.	
10.3	Are applications and systems up-to-date with appropriate vulnerability patches and software updates prior to implementation?	Yes	When deployed, Surgimap support will install the most up to date version including all patches.	
10.4	Is there an established process for notifying customers when a security update, patch or hotfix needs to be installed?	Yes	Surgimap is class II medical device and as such has established quality systems and procedures to notify customers for the security updates. The software will automatically update and in addition Surgimap can force updates or disable accounts when needed.	
10.5	Do you have an SLA for patching? Please provide your SLA for patching.	N/A	Surgimap pushes updates real-time, 7 days a week when available.	

11. Application and System Logging

Item	Question	Yes / No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
11.1	Are all server modifications logged? If so how long are the logs retained?	N/A	Surgimap is desktop software.	
11.2	Are all database modifications logged? If so how long are the logs retained?	Yes	All Surgimap desktop database changes are stored locally with logs.	
11.3	Are all configuration changes to the application logged? If so how long are the logs retained?	N/A	Surgimap is a desktop application. Our logs indicate which version a user is currently on as well as when they upgraded to a newer version.	
11.4	Do logs recording application access, modification and deletion of confidential information contain all of the below elements?			
11.5a	Date and time stamp?	Yes	Surgimap records the timestamp of login and log out. All Surgimap Access modification and deletions are tracked with timestamp.	
11.5b	Location of access (IP address, local, etc.)	Yes	Yes, Surgimap can track location of access when users are connected online. Location of country, state and city using IP address lookup tables. Our data is at IP level.	
11.5c	Identity of the person whose	Yes	Surgimap tracks this at multiple locations, e.g., when users	

	record was accessed?		connect to Surgimap to PACS, when using Surgimap Access.	
11.5d	Identity of individual accessing the record?	Yes	Surgimap can only be used after user login. All stats/user logs are at the individual level.	
11.5e	Specific content within the record that was accessed?	Yes	Yes, Surgimap can track which images were opened/viewed. This data is only available for Surgimap Access. Other Surgimap content logs are based on login/log out and actions taken.	
11.5f	Changes made to the record including deletion?	Yes	All changes for Surgimap are at the record level (save/delete implant templates and images) and include deletion tracking with timestamp.	
11.6	Can the logs be altered or deleted? If so by who?	No	All logs are stored and kept in accordance with HIPAA guidelines. They cannot be altered or deleted.	

Hosted Data Security

Networking and Server Security

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
12.1	Is the hosted environment configured with a firewall at the perimeter and a firewall separating DMZ from any internal zones?	Yes	Surgimap desktop application can synchronize to Surgimap Access (a cloud version of Surgimap). The desktop version is installed behind the Hospital firewall on the Hospital computers. The online version is hosted at Amazon AWS.	
12.2	Are vulnerability scans and penetration tests performed on a	Yes	We rely on Hospital vulnerability scans and penetration test to ensure Hospital computers are secure. The Surgimap desktop version has its own brute force blocking as well as	

	regular basis?		256-bit encryption throughout. The online Surgimap Access is hosted at Amazon AWS with its own vulnerability scans and penetration tests. Details can be found on the AWS-Security-Whitepaper.pdf document.	
12.3	Do you have an established SLA for fixing any vulnerabilities discovered?	Yes	Surgimap processes and methodologies ensure ongoing fixes for any vulnerabilities discovered. These fixes are deployed as per FDA and HIPAA guidelines.	
12.4	Has your application been subject to 3rd party penetration testing? If yes, please describe your pen testing methodology.	No	Surgimap has not had any official/documented third party penetration testing. However, many of our existing hospital relationships have conducted their own testing and all recommendations have been implemented, e.g., changes in password complexity, brute-force lock out.	
12.5	Have all findings for the 3rd party penetration testing been mitigated?	Yes	Surgimap has implemented all findings reported. We actively work with our partners to identify and mitigate any vulnerabilities.	
12.6	Does the configuration of the service prohibit storing confidential data in the DMZ or any external-facing network zone?	Yes	Surgimap can be configured to only operate within the hospital network or restricted to a single Hospital computer. We do not limit surgeons, however work with hospital regulatory/compliance to configure the service offering, as per Hospital policy.	
12.7	Are network intrusion detection and prevention system in place?	Yes	In addition to Hospital detection and prevention, Surgimap desktop blocks brute-force logins when in hospital mode. The online Surgimap Access running on Amazon AWS meets the AWS security standards. More detail can be found on AWS-Security-Whitepaper.pdf document.	

12. Data Center Security

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
13.1	Has the data center deployed physical security controls such as card control entry, staffed reception area, and security cameras?	Yes	Surgimap is a desktop application running on Hospital computers. Patient images stored in Surgimap within the embedded Surgimap database are only accessible to users who authenticate onto the Hospital computer and subsequently login to the Surgimap application. We rely Hospital physical security controls to restrict unauthorized computer access. For those using the Surgimap Access cloud feature, the Amazon AWS data center has comprehensive physical security controls. More detail can be found on AWS-Security-Whitepaper.pdf document.	
13.2	Is physical access to the data center logged?	Yes	Hospital has its own physical access controls regarding computer use where Surgimap is installed. For those using the Surgimap Access cloud feature, the Amazon AWS data center has logs regarding physical access. More detail can be found on AWS-Security-Whitepaper.pdf document.	
13.3	Is sensitive or mission critical data backed-up on a regular basis?	Yes	The Surgimap desktop application funs on Hospital computers. Data within Surgimap is secondary (PACS is primary source). If Hospital does not backup the computer, then users can back up their data to our cloud (Surgimap Access). For those using the Surgimap Access cloud feature, our Amazon AWS solution has comprehensive backups. More detail can be found on AWS-Security-Whitepaper.pdf document.	
13.4	Are backups containing customer data encrypted and stored offsite?	Yes	For those using the Surgimap Access cloud feature, our Amazon AWS solution has comprehensive backups. All Surgimap data including backups is fully encrypted and	

			password protected. More detail can be found on AWS-Security-Whitepaper.pdf document.	
13.5	Does the data center have an incident response plan in case of a breach or environmental issue?	Yes	Surgimap desktop application with the embedded Surgimap database running on Hospital computers relies on Hospital response plan. For those using the Surgimap Access cloud feature, our Amazon AWS solution has incident response plans. More detail can be found on AWS-Security-Whitepaper.pdf document.	
13.6	Are data centers used to store Hospital data located **only** within the United States?	Yes	Surgimap data is stored locally within the embedded Surgimap database on Hospital computers. For those using the Surgimap Access cloud feature, our Amazon AWS solution has is located only within the United States.	

13. Personnel and Administrative Security

Item	Question	Yes No	Vendor Comments (No or N/A answers will require an explanation)	Hospital Comments
14.1	Do all employees undergo security and privacy awareness training?	Yes	Surgimap is a medical device. All employees are required to undergo comprehensive HIPAA training, including security and privacy awareness.	
14.2	Does the vendor have dedicated information security staff?	Yes	Surgimap Information Security is under the control of our General Counsel.	
14.3	Do all employees have their own unique login?	Yes	All Surgimap employees have their own credentials for login.	
14.4	If vendor is a Business Associate based on the HIPAA definition, are	Yes	Surgimap is a medical device and adheres to all HIPAA guidelines. Surgimap can only be accessed by users who are registered. The registration process includes acceptance	

	business associates agreements in place with all downstream subcontractors that may have access to Hospital data?		to a Business Associates Agreement. Any downstream subcontractors that may want access to the Surgimap data must create and register their own account.	